Authentication Formats for UAS

draft-wiethuechter-tmrid-auth-03 Adam Wiethuechter

TMRID BOF – IETF 106 - November 19th, 2019

Background

- ASTM Standard from F38 Committee
 - WK65041: New Specification for UAS Remote ID and Tracking
 - Passed ballot Nov 7th, will become available soon
- Authentication message
 - 5 pages long with a 109 byte max payload (17 + 23 * 4)
 - Design driven to authenticate atomic message and carry certs

0								1										2											2	
01	2	34	5	6	5 7	8	9	0	1	2	3	4	5	6	78		9	2 01	2		3	4	5	(6	7	8	9	9 0	1
A	STM	He	ac	ler	·	+- +	AS	ать 	1 4	\ut	:he	ent	tio	at:	ion	-		ade	rs	-	+ +-	- ·								
						A	utł	ner	nti	ica	ati	ior	n [Dat	a /		Si	gna	tu	r	e									
age	1		•••													-				-										
0 0 1	2	34	5	5 E	5 7	8	9	1 Ø	1	2	3	4	5	6	78		9	2 01	2		3	4	5	(6	7	8	9	3 Ø	-
0 0 1 	2 STM 	4 3 4 Hea	 ac	ier	5 7	' 8 +- +	9	1 0	1	2	3	4	5	6	78	_	9	2 0 1	2	-	3 	4	5	(6	7	8	9	3 Ø 	
0 01 A 	2 STM	3 4 Hea	 ac	5 6 	5 7	' 8 +- +	9 	1 0 :	1 	2 	3	4 	5 	6 Da	7 8 	/	9 S	2 0 1 	2 	u	3 	4	5		5	7	8	9	3 0 	_

D--- 0.

Bluetooth Background

- Why so small?
 - Bluetooth 4 legacy frames only give 25 bytes to play with (after Bluetooth headers)
 - 1 byte is for a main header in Open Drone ID (ODID) that is always present – now only 24 bytes
 - Auth message has its own header + other fields



HIP Based Authentication Wrapper

- HHIT can be looked up to obtain HI from DNS, thus allowing verification of HHIT being genuine
- Payload is used to generate Signature
 - Must have some sort of dynamic field in data to be signed, Trust Timestamp could be used for this if Payload static
- Signature can be verified using HI + Auth message fields



Trusted [Vector] Message

- Base format (left image)
- An example using Vector message (right image)
 - Vectors are dynamic so at minimum just the 25 byte Payload needs to be signed
- Prototype of format developed at AX Enterprize
 - Currently only the send side of operation with manual verification test



Signed Hash Lists

- Provides provenance to previously sent messages (left image)
 - Agility through H-Alg and H-Len fields
 - Pseudo-blockchain hashes to link signed lists together
- Could also use idea in wrapper format (right image)
 - Removes pseudo-blockchain hashes, lowers count
- Is the number of hashes worth it?

age ø:				Page 0:		
01234567	1 89012345	67890123	4567890	L 0 1 2 3 4 5 6	1 7 8 9 0 1 2 3 4 5 6 7 8	$\begin{smallmatrix}&2\\9&0&1&2&3&4&5&6&7&8&9&0\end{smallmatrix}$
ASTM Header	+ ASTM Authenti	cation Headers		ASTM Header	ACTH Authoritication	Handans
			H-Alg H-Len		-+ ASIM Authentication	RESERVED
	Hash of Previou	s Auth. Message		1		
	Hash of Current	Auth. Message				
	Messa	ge Hash		-+ 	HHIT	
	Messa	ge Hash		-+ -+ +		
Page 1.				Dage 1		
0 1 2 3 4 5 6 7	1 8 9 0 1 2 3 4 5	2 67890123	3 4 5 6 7 8 9 0 3	0 0 1 0 1 2 3 4 5 6	1 7 8 9 0 1 2 3 4 5 6 7 8	2 9 0 1 2 3 4 5 6 7 8 9 0
ASTM Header	H-Alg H-Len	RES	ERVED	ASTM Header	Trus	t Timestamp
	Messa	ge Hash		1 /	RESERVED	
	Messa	ge Hash		+ +	-++	
	Messa	ge Hash		-+ 		
	Messa	ge Hash		-+ 	HHIT Signatu	re
	Messa	ge Hash		-+		
				+ +		
Page 2: 0	1	2	3	Page 2: 0	1	2 3
01234567	89012345	67890123	4567890	0123456	789012345678	901234567890
ASTM Header	RESERVED	Signatur	e Length	ASTM Header	-+	
Signature	e Algorithm					
		+				
					HHIT Signatu	re
	HHIT S	ignature				
				-+ +		
Page 3: 0	1	2	3	Page 5. 0	1	2 3
01234567	89012345	67890123	4567890:	-+ +	189012345078	901234567890
ASTM Header	+			ASIM Header	-+	
	HHIT S	ignature			HHIT Signatu	re
				Page 4		
Page 4: 0	1	2	3	0	1	2 3
01234567	89012345	67890123	4567890	+ +		901234507890
ASTM Header	 +			ASTM Header	M-A1g H-Len	KESERVED
					Message Has	n
					Message Has	h
	HHIT S	ignature			Message Has	h
					Message Has	h
					Message Has	h
				+		

HIP Based Offline Authentication

- Currently unobtainable with ASTM format
 - Need at least 10 pages, not 5 pages
- DEV side
 - HHIT and Signature validation can be done without any lookups
- AUTH side
 - Registry HHIT and SIG to show, without lookup, the registry UA belongs in
 - Local cached list of Registries on Observer device
 - Trust can be asserted from information if desired
- Further lookups and validation once connectivity restored for Observer



Future Work Needed

- Work with ASTM on expanding 5 pages to 10 pages
 Format might migrate into ASTM instead of staying in IETF
- Format; improvements?
- Draft work
 - Security/IANA Considerations
 - Missing prose anywhere?
- Development of prototypes
 - Wrapper Message (receive side)
 - Signed Hash Lists



Q&A



Questions, Comments, Concerns?

"Today's consumers who order their drones off the internet don't know the joy of going out in nature and returning with a drone that you caught yourself, whose angry owners you fought off with your own two hands." https://xkcd.com/2208/

Backup Slides

